§170.315(g)(7) Application access — patient selection

2015 Edition CCGs

Version 1.7 Updated on 06-15-2020

Revision History		
Version #	**Description of Change**	**Version Date**
1.0	Initial Publication	10-26-2015
1.1	Header information updated. Revisions made to remove Designated Record Set and HIPAA Security rule references. Third-party API development clarification added. Terms of use documentation and hyperlink clarifications added.	03-22-2016
1.2	Added clarification in the 'applies to entire criterion section' related to the product update requirements.	11-09-2016
1.3	Added clarification on API Registration requirements and removed guidance on API registration mechanism (dynamic registration). Added clarification on the definition of a "trusted connection".	07-07-2017

1.4	Added clarification for paragraph (g)(7)(ii)(B) that documentation must be available to the public via a hyperlink without any additional access requirements.	08-25-2017
1.5	Revised clarification for paragraph (g)(7)(ii)(B) that the hyperlink provided for all of the documentation must reflect the most recent version of all the documentation, not just the terms of use.	09-29-2017
1.6	Made revisions to a prior clarification in (g)(7)(ii)(A)(*3*) regarding the terms of use. Added a new clarification for paragraph (g)(7)(ii)(A)(*3*) regarding enforcement of the health IT developer's terms of use, which is out of scope for this criterion. Additionally, noted CMS' guidance that providers may not prohibit patients from using the app of the patient's choice.	02-01-2018
1.7	Updated the Security requirements per 21st Century Cures Act.	06-15-2020

Regulation Text

Regulation Text

§170.315 (g)(7) *Application access – patient selection—*

The following technical outcome and conditions must be met through the demonstration of an application programming interface (API).

    (i) *Functional requirement.* The technology must be able to receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient's data.

    (ii) *Documentation—*
        (A) The API must include accompanying documentation that contains, at a minimum:
            (1) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
            (2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).
            (3) Terms of use. The terms of use for the API must be provided, including, at a minimum, any associated developer policies and required developer agreements.
        (B) The documentation used to meet paragraph (g)(7)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced
None

Certification Companion Guide: Application access — patient selection

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is <u>not</u> a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
New	No	Included	Yes

Certification Requirements

<u>Privacy and Security</u>: This certification criterion was adopted at § 170.315(g)(7). As a result, an ONC-ACB must ensure that a product presented for certification to this criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be presented once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "VDT" and (e)(2) "secure messaging," which are explicitly stated.

- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

Table for Privacy and Security

- If choosing Approach 1:
  - Authentication, access control, and authorization (§ 170.315(d)(1))
  - Trusted connection (§ 170.315(d)(9))
  - Either auditable events and tamper-resistance (§ 170.315(d)(2)) or auditing actions on health information (§ 170.315(d)(10)).
  - Encrypt Authentication Credentials (§ 170.315(d)(12))
  - Multi-factor Authentication (MFA) (§ 170.315(d)(13))
- If choosing Approach 2:
  - For each applicable P&S certification criterion not certified for approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule at 85 FR 25642 for additional clarification.

Design and Performance: The following design and performance certification criteria (adopted in

§ 170.315(g)) must also be certified in order for the product to be certified.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- While no standard is required for this criterion, we intend to adopt a standards-based approach for certification in a future rulemaking. We encourage the use of the Fast Healthcare Interoperability Resources (FHIR) specification.
- *Security:*
  - For the purposes of certification there is no conformance requirement related to the registration of third party applications that use the APIs. If a Health IT module requires registration as a pre-condition for accessing the APIs, then, the process must be clearly

specified in the API documentation as required by the criterion. We strongly believe that registration should not be used as a means to block information sharing via APIs.

- This criterion does not currently include any security requirements beyond the privacy and security approach detailed above, but we encourage organizations to follow security best practices and implement security controls, such as penetration testing, encryption, audits, and monitoring as appropriate. We expect health IT developers to include information on how to securely use their APIs in the public documentation required by the certification criteria and follow industry best practices. [see also 80 FR 62676]
- We strongly encourage developers to build security into their APIs following best practice guidance, such as the Department of Homeland Security's Build Security In initiative.[1] [see also 80 FR 62677]
- A "trusted connection" means the link is encrypted/integrity protected according to § 170.210(a)(2) or (c)(2). As such, we do not believe it is necessary to specifically name HTTPS and/or SSL/TLS as this standard already covers encryption and integrity protection for data in motion. [see also 80 FR 6267]
- APIs could be used when consent or authorization by an individual is required. In circumstances where there is a requirement to document a patient's request or particular preferences, APIs can enable compliance with documentation requirements. The HIPAA Privacy Rule[2] permits the use of electronic documents to qualify as writings for the purpose of proving signature, e.g., electronic signatures. [see also 80 FR 62677]

- By requiring that documentation and terms of use be open and transparent to the public by requiring a hyperlink to such documentation to be published with the product on the ONC Certified Health IT Product List, we hope to encourage an open ecosystem of diverse and innovative applications that can successfully and easily interact with different Health IT Modules' APIs. [see also 80 FR 62679]
- A health IT developer must demonstrate that its API functionality properly performs consistent with this certification criterion's requirements. How this is done is up to the health IT developer. Doing so could include, but is not limited to, the health IT developer using existing tools or creating its own app or "client" to interact with the API as well as using a third-party application.
- Health IT developers are able to update/upgrade/improve functionality that's within the scope of certification, provided that certain rules and conditions are followed. The "API criteria" § 170.315(g)(7), § 170.315(g)(8), and § 170.315(g)(9) are treated no different under this regulatory structure. If a developer seeks to update their API functionality post-certification a developer will need to consider the following:
  - If their ONC-ACB requires notification or updated documentation associated with the functionality they changed. This procedure is at the discretion of the ONC-ACB and may result in an additional CHPL listing.
  - Pursuant to the certification criteria, there is a documentation portion in each. Which would include (publicly available) technical specs, configuration requirements, and terms of use. Insofar as a developer updates their API post-certification, they are expected to keep all of this documentation up-to-date. Similarly, ONC-ACBs are expected to oversee/enforce/surveil that this action is taken and could find a non-conformity if those updates are not made.
  - If any of their changes would require updates to the developer's 170.523(k)(1) disclosures (the broader product transparency disclosures).

---

[1] https://buildsecurityin.us-cert.gov/

[2] 45 CFR Part 160 and Part 164, Subparts A and E

Paragraph (g)(7)(i)

Technical outcome – The health IT can receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient's data.

Clarifications:
- The developer can determine the method and the amount of data by which the health IT uniquely identifies a patient. [see also 80 FR 62678]
- The term "token" is not to be interpreted as the token in the OAuth2 workflow, but simply as an identifier for something that would uniquely identify a patient.

Paragraph (g)(7)(ii)(A)(*1*)

Technical outcome – The API must include accompanying documentation, which contains API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions, and exception handling methods and their returns.

Clarifications:
- No additional clarifications available.

Paragraph (g)(7)(ii)(A)(*2*)

Technical outcome – The API must include accompanying documentation, which contains software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

Clarifications:
- No additional clarifications available.

Paragraph (g)(7)(ii)(A)(*3*)

Technical outcome – The API must include the terms of use for the API including, at a minimum, any associated developer policies and required developer agreements.

Clarifications:
- Health IT developers must be clear and transparent about the general terms of agreements or contracts that will typically apply to all prospective third-party applications.
- Health IT developers that typically execute unique agreements or contracts with interested third-party applications using their API must disclose this practice as part of their terms of use.
- For the purposes of certification, a health IT developer is accountable for documenting and making public the provisions of its API's terms of use. If, post-certification, a health IT developer permits its customers to deploy and integrate its API in ways where the customer would be able to layer on its own specific terms of use unique to that organization, the health IT developer would need to disclose this business practice in its terms of use. A health IT developer is NOT expected to change or factor

instances into its terms of use where its customers establish additional, organizational-specific terms for the API's use.

- Pursuant to the certification criterion's documentation requirement, health IT developers are required to make their API documentation publicly available, including terms of use (and its associated policies and required developer agreements). Developers' enforcement of their terms of use is beyond the scope of conformance to this certification criterion. This criterion focuses on the technical API capabilities with which a Health IT Module must be in compliance and documentation requirements as specified. For example, this certification criterion does not require health IT developers to evaluate app developers or prohibit such activity (though such activities may implicate other requirements of the Program). We also note that CMS, specifically in the patient access context, states that "[p]roviders may not prohibit patients from using any application, including third-party applications, which meet the technical specifications of the API, including the security requirements of the API."[3]

---

[3] https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/MedicaidEPStage3_Obj5.pdf

Paragraph (g)(7)(ii)(B)

Technical outcome – The documentation used to meet the provisions in (g)(7)(ii)(A)(*1*)-(*3*) must be available through a publicly accessible hyperlink.

Clarifications:

- The hyperlink provided for all of the documentation referenced by provision (g)(7)(ii)(A) must reflect the most current version of the Health IT developer's documentation.
- All of the documentation referenced by provision (g)(7)(ii)(A) must be accessible to the public via a hyperlink without additional access requirements, including, without limitation, any form of registration, account creation, "click-through" agreements, or requirement to provide contact details or other information prior to accessing the documentation.

Content last reviewed on June 23, 2020